the IG

FRAUD ALERT

April 2020

KEN BURKE
CLERK OF THE CIRCUIT COURT
AND COMPTROLLER

You Have A VOICE Report Cybercrime

FRAUD ALERT

SIGN UP TODAY and receive free alerts when a document with your name is recorded in Official Records. Protect yourself from fraud. **CLICK HERE.**

GET IN TOUCH:

Write:
Public Integrity Unit
Division of Inspector General
Fraud Hotline
510 Bay Avenue
Clearwater, FL 33756

Call:
(727) 45FRAUD
(727) 453-7283
Fax:
(727) 464-8386
E-mail:
fraudhotline@mypinellasclerk.org
Internet:
www.mypinellasclerk.org
www.twitter.com/pinellasig
www.facebook.com/igpinellas

Coronavirus Related Fraud Schemes

Serial fraudsters think differently than the rest of us. They do nothing but sit around and come up with new ways to defraud people. Natural disasters are a perfect time to strike.

During the Coronavirus, consumers, businesses, and government may be more vulnerable and can easily fall victim to scams related to the pandemic. Unlike natural disaster schemes that involve property damage and contractor fraud, Coronavirus scammers focus on cyber fraud, fraudulent products, investment fraud/pump-and-dumps, and charity fraud to name a few. As government, law enforcement, and regulatory fraud controls halt as operations are limited to essential personnel, worldwide data security stalls as companies shift focus to virus response, and millions of consumers are stuck at home with Coronavirus worries, all are more vulnerable to the following attacks.

Coronavirus Phishing and SMiShing

- Phishing is any fraudulent communication that purports to be from a legitimate sender to induce a victim to reveal financial data, email credentials, etc.
- SMiShing is similar to phishing, but uses short message service (SMS) text messages instead of email.
- Phishing emails are spoofed and imply to be from the Centers for Disease Control and Prevention (CDC) or World Health Organization (WHO).
- Phishing emails route the user to a fake email login page to enter their email credentials. The email and password are stored for the cybercriminals' later use.
- Phishing emails typically include language to elicit fear and urgency from the victim.
- Multiple websites have reported SMiShing scams that use a variety of techniques to get the victim to click on a link, such as:
  - Offering products, such as free masks or iPhones.
  - Impersonating the CDC or WHO.
  - Demanding money from a business for a sender who claims that they have contracted COVID-19 from the victim's business.
  - Faking FedEx texts asking the user to update their delivery preferences to protect from COVID-19.
- To protect yourself against phishing and SMiShing:
  - Be wary of unsolicited emails or SMS text messages offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the public this way.
  - Do not click on links, open email attachments, or download files from unknown or unverified sources. Doing so could download a virus onto your computer or device.
  - Make sure the anti-malware and anti-virus software on your computer are operating and up-to-date.

Product Scams

- Watch out for sellers on legitimate commerce sites, such as Amazon and Walmart, which redirect to a third-party site for purchases.
- If the seller wants to be paid in cryptocurrency, this could be a red flag.
- Amazon alone claims it has removed more that 1 million products over fraudulent COVID-19 claims or price gouging.
- Remember, there are currently no legitimate COVID-19 vaccines and the WHO is not distributing any such vaccine.
- To protect yourself against product scams:
    - Pay with credit cards, which have more protection than debit cards.
    - Do not pay in cryptocurrency if asked.

Corporate Fraud (External)

- Business email compromise schemes generally feature some sense of urgency in redirecting a payment.
- With everyone working remotely in uncertain economic conditions, requests can seem very real.
- Remember, requests are not always for a payment; sometimes they are for Human Resources information, such as W2s.
- To protect your business against external corporate fraud:
    - Verify any change in payment instructions.
    - Check trusted sources of information regularly and ignore unsolicited emails.
    - If possible, verify requests via phone calls to known numbers.
    - Do not rush any transactions.

Corporate Fraud (Internal)

- With typical business conditions interrupted or strained, fraudsters might consider that their risk of detection is low putting the business at risk for:
    - Expense fraud
    - Payroll schemes (e.g. ghost employees and time-card fraud)
    - Misappropriation of assets
    - Inventory theft
- Do not lose sight of fraud detection because of irregular operating conditions.
- Be aware of remote-working vulnerabilities and ensure:
    - Employees have secure virtual private networks.
    - Designated Information Technology (IT) helplines are available that employees can call to avoid tech-support scams.
    - Adequate resources so IT will not be too swamped with remote-working troubleshooting to monitor anti-fraud controls and processes.
    - External emails are automatically marked in a clear fashion.

Investment Fraud

- Fraudsters are looking to capitalize on economic uncertainty, crashing stock markets, and general Coronavirus chaos.
- Be cautious of penny stocks involving companies supposedly finding cures. These claims may be made as part of fraudulent "pump-and-dump" schemes in which fraudsters spread false or misleading information to create a buying frenzy that will "pump" up the price of a stock and then "dump" share of the stock by selling at the inflated price.
- Be cautious of prompts to buy in to any cryptocurrencies or precious metals while the stock market is down.
- Be cautious of fake celebrity endorsements of products such as, "Tom Hanks loved this treatment in quarantine."
- Submissions of tips, complaints, or referrals relating to suspected securities fraud or wrongdoing can be made online at https://www.sec.gov/tcr.

FRAUD ALERT

Charity & Crowdfunding Scams

- While there are no concrete examples (yet), fake charity scams go hand-in-hand with natural disasters.
- Fraudsters solicit donations for non-existent charities or charitable situations on crowdfunding sites such as GoFundMe and KickStarter.
- To protect yourself against fake charity scams:
  - Do your homework; there are many sites such as Charity Navigator https://www.charitynavigator.org/ to help research charities.
  - Pay by credit card or check. If they want cash, gift cards, wires, or bitcoin, those are red flags for scammers.
  - Do not let anyone rush you into a donation. Scammers will be very good at tricking you into thinking you are dealing with a legitimate charity. They will often use familiar charity names.

Price Gouging

- While not exactly fraud, price gouging is the (usually illegal) act of increasing the price of goods or services to levels much higher than reasonable in a given market.
- This scheme usually coincides with a disaster or other increase in demand.
- To report price gouging in Florida, you may visit http://myfloridalegal.com/ or call the hotline at 1-866-9-NO-SCAM (866-966-7226).

Source: Jason Zirkel, CFE, Training Director, Association of Certified Fraud Examiners (ACFE)

The U.S. Attorney's Office for the Middle District of Florida is launching a Coronavirus fraud task force. Investigators will target fake cure, fake charities, cyber-extortion, and scams targeting people's stimulus payments.

To report a suspected Coronavirus fraud, call toll-free 1-866-720-5721 or email disaster@leo.gov.

Source: Tampa Bay Times

Pinellas County CONSUMER PROTECTION

For more information or to file a complaint, contact Pinellas County Consumer Protection at (727) 464-6200 or visit www.pinellascounty.org/consumer.